Arithmétique 2

Les congruences

Nicole MONTENEGRO

Septembre 2017

Sommaire

Vous passez l'épreuve de SI9 (Compétences artistiques) à l'oral devant un des 9 jurys.

Vous êtes le candidat n° 331 sur la liste.

Avec quel jury (numéroté de 1 à 9) allez vous passer ?

Votre copain n° 286 est il sur le même jury ?

$$\begin{aligned} 331 &= 36 \times 9 + 7 \\ 331 - 286 &= 9 \times 5 \end{aligned}$$

$331 - 7$, $331 - 16$ et $331 - 286$ sont des multiples de 9. 331 est à plusieurs multiples de 9 (pas de 9) des entiers 7, 286 et 16.

Définition

Soient a et b deux entiers. Soit p un entier, $p \geqslant 2$.
On dit que

a est congru à b modulo p si $a - b$ est un multiple de p.

On note alors

$$a \equiv b[p] \qquad \text{ou encore} \quad a \equiv b \bmod p.$$

Sommaire

$17 \equiv 8[3]$ car $17 - 8 = 9$, et 9 est multiple de 3,

$23 \equiv 2[3]$ car $23 - 2 = 21$ et $21 = 3 \times 7$,

$23 \equiv -1[3]$ car $23 - (-1)$ est multiple de 3.

Propriété

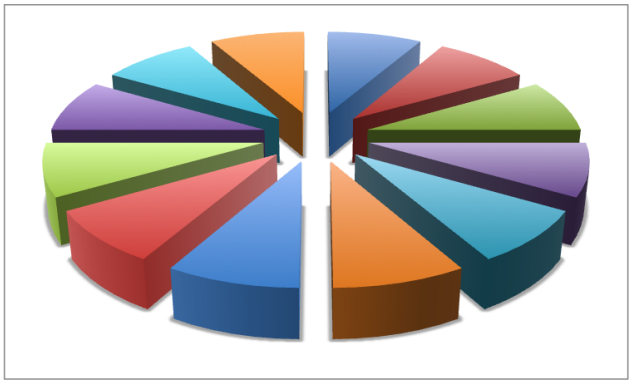
a est congru à b modulo n si a et b ont même reste dans la division euclidienne par n.

On remarquera que a est un multiple de b ssi $a \equiv 0[b]$.
Ainsi,

$$a \text{ est pair ssi } a \equiv 0[2].$$

$$a \text{ est multiple de } 5 \text{ ssi } a \equiv 0[5].$$

Applications :



Une puce se trouve sur la case 0 d'un plateau circulaire de 12 cases.

1. Supposons qu'elle ait avancé de 15 sauts de 2 cases ; sur quelle case va-t-elle se poser ?
2. Si elle a fait 31 sauts de 3 cases, où atterit-elle ?

1. Supposons qu'elle avance par sauts de 2 cases ; sur quelles cases va-t-elle se poser ?
2. Si elle fait des sauts de 3 cases, quelles sont les cases qu'elle occupera ?
3. Peut-elle passer sur toutes les cases du plateau autrement qu'avec des sauts de 1 case ?
4. Si le plateau comportait 15 cases, quels sauts lui permettraient de visiter chaque case ?

Sommaire

Définition

Exemple

Propriétés

À retenir

Propriété

La relation de congruence modulo p est compatible avec les opérations algébriques usuelles :

Si $a \equiv b[p]$ *et* $a' \equiv b'[p]$ *alors*

$$\begin{aligned} a + a' &\equiv b + b' \ [p] \\ n \times a &\equiv n \times b \ [p] \\ a \times a' &\equiv b \times b' \ [p] \\ a^k &\equiv b^k \ [p] \end{aligned}$$

pour tout entier n et pour tout entier naturel non nul k.

Exemples :
Quel est le reste dans la division euclidienne par 6 de 2015^{2015} ?

$$2015 = 335 \times 6 + 5$$

$$\text{donc} \quad 2015 \equiv 5[6]$$

Par compatibilité de la relation de congruence avec la puissance,

$$2015^{2015} \equiv 5^{2015}[6]$$

Exemples :

Quel est le reste dans la division euclidienne par 6 de 2015^{2015} ?

$$2015 = 335 \times 6 + 5$$

$$\text{donc} \quad 2015 \equiv 5[6]$$

Par compatibilité de la relation de congruence avec la puissance,

$$2015^{2015} \equiv 5^{2015}[6]$$

Exemples :
Quel est le reste dans la division euclidienne par 6 de 2015^{2015} ?

$$2015 = 335 \times 6 + 5$$

$$\text{donc} \quad 2015 \equiv 5[6]$$

Par compatibilité de la relation de congruence avec la puissance,

$$2015^{2015} \equiv 5^{2015}[6]$$

mais aussi

$$2015^{2015} \equiv (-1)^{2015}[6]$$

$$\text{car} \quad 5 \equiv -1[6]$$

or

$$(-1)^{2015} = -1$$

donc

$$2015^{2015} \equiv -1[6]$$

ou

$$2015^{2015} \equiv 5[6]$$

Dans la division euclidienne par 6 de 2015^{2015}, le reste est égal à 5.

mais aussi

$$2015^{2015} \equiv (-1)^{2015}[6]$$

$$\text{car} \quad 5 \equiv -1[6]$$

or

$$(-1)^{2015} = -1$$

donc

$$2015^{2015} \equiv -1[6]$$

ou

$$2015^{2015} \equiv 5[6]$$

Dans la division euclidienne par 6 de 2015^{2015}, le reste est égal à 5.

mais aussi

$$2015^{2015} \equiv (-1)^{2015}[6]$$

$$\text{car} \quad 5 \equiv -1[6]$$

or

$$(-1)^{2015} = -1$$

donc

$$2015^{2015} \equiv -1[6]$$

ou

$$2015^{2015} \equiv 5[6]$$

Dans la division euclidienne par 6 de 2015^{2015}, le reste est égal à 5.

mais aussi

$$2015^{2015} \equiv (-1)^{2015}[6]$$

$$\text{car} \quad 5 \equiv -1[6]$$

or

$$(-1)^{2015} = -1$$

donc

$$2015^{2015} \equiv -1[6]$$

ou

$$2015^{2015} \equiv 5[6]$$

Dans la division euclidienne par 6 de 2015^{2015}, le reste est égal à 5.

Un entier est pair si son chiffre des unités est pair.*

En effet, si $n \in \mathbb{N}$,

$$n = a_k 10^k + \ldots + a_2 10^2 + a_1 10 + a_0$$

où a_0 est le chiffre des unités, a_1 celui des dizaines, a_2 celui des centaines ...

$$\begin{aligned} 10^k &\equiv 0[2] \\ 10^2 &\equiv 0[2] \\ 10 &\equiv 0[2] \end{aligned}$$

Donc

$$n \equiv a_0[2] \ !^*$$

Un entier est multiple de 9 si la somme de ses chiffres est multiple de 9.

$$
\begin{aligned}
10 \equiv 1[9] \quad &\Rightarrow \quad 10^2 \equiv 1^2[9] \\
&\Rightarrow \quad 10^2 \equiv 1[9] \\
&\Rightarrow \quad 10^3 \equiv 1^3[9] \\
&\Rightarrow \quad 10^3 \equiv 1[9] \\
&\dots \\
&\Rightarrow \quad 10^k \equiv 1[9]
\end{aligned}
$$

Ainsi, pour

$$n = a_k 10^k + \ldots + a_2 10^2 + a_1 10 + a_0$$

$$n \equiv a_k + \ldots + a_2 + a_1 + a_0 [9] \text{ !}$$

Un entier est congru à la somme de ses chiffres modulo 9.

Si cette somme est multiple de 9, cet entier le sera aussi.

Le nombre 6 439 817 263 459 653 est il divisible par 9 ?

Propriété

Modulo n, les multiples de a sont les multiples du PGCD(a, n).

Les multiples de 2 modulo 12 sont les multiples de PGCD(2,12) c'est à dire les multiples de 2 : 0, 2, 4, 6, 8, 10

Les multiples de 3 modulo 12 sont les multiples de PGCD(3,12) c'est à dire les multiples de 3 : 0, 3, 6, 9

Les multiples de 5 modulo 12 sont les multiples de PGCD(5,12) c'est à dire les multiples de 1 : 0, 1, 2, 3, …11

Sommaire

Définition

Exemple

Propriétés

À retenir

Soient a et b deux entiers. Soit p un entier, $p \geqslant 2$. On dit que

a est congru à b modulo p si

Notation :

Quel lien existe-t-il entre la relation de congruence et le reste dans la division euclidienne ?

La relation de congruence modulo p est compatible avec les opérations algébriques usuelles :